

Two protocol approaches come immediately to mind. The first entails establishing a fixed timing clock for the whole network grid, and then making each node responsible for synchronizing its interactions with the network by the universal clock. This approach is the simplest to implement, it is also the least flexible. The second option involves using a routing header to direct the qubit to its destination node. Unlike the header for the standard TCP/IP protocols, qubit headers must explicitly include time slot or time tag information. This is especially

important when routing headers are used in MAN and WAN networks, because the arrival time will appear random from the perspective of the receiving node. What are the implications for distributing qubits about a network? The initial assumption is that the qubits will be routed within a local area network (LAN) environment. However, ultimately, one needs to be able to scale up to an arbitrarily large number of nodes. This implies that one must ultimately have the ability to link multiple LAN's together and to institute a protocol that facilitates the ability to pass qubits among them.

The temptation is to adapt something similar to the OSI (Open Systems Interconnection) protocol that has proved a spectacular success for the internet. If that is done, one is immediately faced with important issues that must be addressed to make OSI protocol quantum compatible. These include but are probably not limited to:

- (1) Routing implications of having a dis-associated header that precedes but is not attached to the qubit
- (2) Physical properties controlling routing (i.e. time-to-live of qubits in network (TTLQ), short-term buffered storage of qubits, decoherence time of the qubits, non-regenerative property of qubits),
- (3) Scaling up from a manageable number of nodes inside LAN,  $n$  (e.g.  $2 < n \leq 20$ ), to  $N$  arbitrarily large, where  $N = Kn \gg n$  and  $K$  is the number of LANs being coupled into the network
- (4) The long term storage of qubits.
- (5) Keeping careful track of each time slot within which the qubit is generated.





All of this assumes that the network protocols for the qubits will be analogous to the first four layers of the standard OSI model. The quantum protocol will follow the TCP/IP (Transmission Control Protocol/Internet Protocol) address routing framework. But when we look at the quantum key distribution (QKD) application for cryptography, we quickly realize that due to (i) the inability to regenerate qubits, (ii) the non-measurement requirement initially placed on the qubit, and (iii) the inability to store photons for indefinite periods of time and/or to recall them on demand, the TCP/IP protocol is not optimized to the quantum features of the qubit. In truth, it is not the only option for qubit distribution and indeed may not be the best. To examine how one might introduce qubits into network applications, let's start with the simple context of evolving from a 2-node fiber link to a 4-node quantum LAN (QuLAN) shown in Fig. 1(b) and understand how the quantum features might be exploited.

### ***Cryptography Application***

The first qubit distribution application to be fielded is Quantum Key Distribution<sup>1</sup> (QKD) application. QKD offers the ability to generate key sequences that can be securely distributed. This is important because the key distribution step is considered to be the weakest part of most classical encryption protocols. QKD combined with the Vernam cipher<sup>2</sup>, offers an unconditionally secure communications protocol.

Within the last few years, QKD in fibers has been demonstrated over distances of several tens of kilometers. In particular, Townsend<sup>3</sup> has not only demonstrated QKD over 30 km of fiber, he has also shown that QKD works quite well when implemented in a conventional Dense Wavelength Division Multiplexed (DWDM) data transmission network. This implies that qubit distribution is currently possible in LAN, MAN, and limited WAN networks. We propose introducing QKD as the first application in our Quantum Internet Testbed, with the idea of extending the use of the testbed to demonstrate a distributed architecture for other Quantum Computing functions as they are developed and matured by other research groups.

Table 1. Alice and Bob's polarization analyzer assignments

| Bit Value | Alice's Polarizer Settings  | Bob's Polarizer Setting   |
|-----------|---|---|
| 0         |  |  |
| 1         |  |  |

*Two-node approach*

Figure 1(a) depicts the classic 2-node network configuration for quantum key distribution. Two parties, Alice, the sender, and Bob, the receiver, want to establish a shared secret by using randomly polarized photons that each of them analyze separately. The protocol they chose (BB84)<sup>4</sup> is implemented as follows:

- (1) Before establishing a shared secret, Alice and Bob must first put into place an infrastructure that allows them to track the time slots,  $t_n$ , into which the  $n$ th photon is generated. As the  $n$ th photon passes through each of their analyzers, first Alice and then Bob make a note of their respective polarization settings for time slot  $t_n$ .
- (2) Alice and Bob both assign 0 and 1 bit values to specific polarization orientations. In doing so, they are careful to select their respective bases so that whenever they select different bit values, their polarizers are always cross polarized so that there is zero probability that a photon will get through. (See for example the assignments in Table 1.) If, on the other hand, they select the same bit value, their polarizers are always offset by 45 degrees with respect to each other. In the latter case, there is a 50% probability that a photon will pass through both polarizers.
- (3) Alice and Bob agree through discussions on a classical channel (radio, phone, etc.) to start their key generation sequence. Each sets their polarization analyzers through a random sequence of zero's and one's at the rate of one bit per time slot.
- (4) Alice has a single photon source that spits out a randomly polarization in each time slot; this photon, of course, is sent to Bob. Before the transmission, however, Alice passes it through her polarization analyzer and makes note of her polarization setting for the time slot. Upon receiving it, Bob, passes the photon through his analyzer before allowing it to impinge on his detector. If he records a photon, he makes note of the timeslot and the value of his polarizer setting. Obviously, when ever Bob receives a photon, he knows absolutely what bit Alices polarizer was set at for that specific timeslot.
- (5) Both Alice and Bob use a classical communications link to agree on a set of bits for the key sequence. In their conversation, Bob essentially tells Alice which time slots he measured a photon from her. Now Alice also knows absolutely the value of Bob's polarization setting for that time slot. By keeping only the bit values of the time slots where Bob was able to make a measurement, they have both agreed on a random string of one's and zero's to use as their encryption key.

To date, most links attempting to distribute qubits connect between two points, A and B (see Figure 1 (a)). Successful qubit delivery is accomplished in these networks with dedicated equipment and the use of timing pulses that precede the qubit and auxiliary communications channels. Quite a bit of overhead beyond the key distribution link is needed to insure the viability of the qubit delivery. In growing from a 2-node network to an N-node network, where  $N > 2$ , one would like to insure that the overhead tends to grow at a slower rate than N.

*Multi-node approach*

There are two approaches that come to mind. One involves the use of an active switch. Ideally, such an expanded quantum distribution network will have features similar to those developed for local area networks, metropolitan area networks, and wide area networks. For example, dynamic routing capability, scalability, and a well defined time-to-live (TTL). Other features will be unique to the quantum distribution network based on the unique physical properties of the qubits. For example, it would require a header dis-associated from the information bearing qubit. Such a header would probably be part of the timing pulse and would potentially need routers capable of reduced header optical packet switching such as those being investigated at UC Santa Barbara, Princeton and MIT Lincoln Labs.<sup>5</sup> Since qubits cannot be regenerated without destroying their quantum properties, this network must handle all routing functions without detecting, regenerating, or amplifying the qubit. Error detection does not have the same meaning when distributing qubits since the state of the qubit is probabilistic. Additionally, specialized routers capable of handling qubits dis-associated from the header and timing pulse need to be developed to ensure appropriate delivery of the qubits. Due to the time delay in reading the header information and configure the node switch, the delivery of the qubits will have to include these and other network latency issues. Thus at all N nodes must be upgraded with additional hardware that is capable of handling the latency. In addition, for each node to establish keys with each other node,  $(N-1)!$  Classical links must be established among the nodes to support the function.

The other option is not to try to control the arrival routing of the qubit at all, but to rely on passive switching (fiber Y-couplers) where the qubit has probability  $a$  of staying in the network and probability  $b$  of coupling out to be analyzed and detected at the node. In this context, after Alice distributes her keys, she gets on phone or radio and chats with each node to find out who received one of her photons in each time slot. In this architecture, the network overhead is concentrated in keeping track of the time slots and in communicating between the nodes during the privacy amplification step. Of course, once the network timing grid is in place, the overhead cost is fixed, no matter how large  $N$  becomes. In contrast, the number of communication links that must be established within any given LAN to complete privacy amplification scales as  $(N - 1)!$  instead of  $N$ .

### ***Distributed Quantum computing***

Finally, we also anticipate that beyond the QKD application, a generalized quantum computer that is capable of more complex functions than key distribution will probably also use a distributed architecture. What we learn here will also lay the groundwork for qubit distribution in distributed quantum computing applications. In particular, passively switched networks described above are very quantum like because their switching protocol is really based on probabilities. We expect to be able to specifically exploit this feature in distributed computing architectures.

### **CONCLUSIONS**

The two major applications that are expected to exploit quantum properties are quantum cryptography and quantum computing. Quantum cryptography derives its essential security from the postulates of quantum mechanics, and does not rely on any presumed technological limitations of an eavesdropper. Quantum cryptography would revolutionize the way secrecy is ensured for both national-interest and commercial communication. Quantum computing uses the entanglement of quantum states to achieve a type of massive parallelism that has no analogy in classical physics. The potential ramifications for space exploration, scientific research, national security, and commercial industry are now recognized to be enormous. Of the two, quantum cryptography is more mature because the hardware exists to allow its implementation as a practical solution to the current key distribution problem. Practical quantum computing, capable of solving problems at a level of complexity that can't be realized by classical methods, still awaits further hardware development. However, we are encouraged by the fact that the trend towards exploiting the measurement properties of quantum systems will yield a breakthrough leading towards practical quantum computing architectures.





### **REFERENCES**

1. C.H. Bennett and G. Brassard, in *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*, IEEE Press, New York (1984); G. Gilbert, and M. Hamrick, "Practical Quantum Cryptography: A Comprehensive Analysis (Part One)", MITRE Technical Report MTR00W0000052, September 2000.
2. G.S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," *J. Amer. Inst. Elect. Eng.* **XLV**, 109-115 (1926).
3. C. Maurand and P. D. Townsend, "Quantum key Distribution Over Distances as Long as 30 km", *Optics Letters* 20, 1695-1697 (1995); P.D. Townsend, "Simultaneous Quantum Cryptographic Key Distribution and Conventional Data Transmission Over Installed Fiber using Wavelength-Division Multiplexing", *Electronics Letters* 33, 188-190 (1997).
4. C.H. Bennett and G. Brassard, in *Proc. IEEE Int. Conference on Computers, Systems, and Signal Processing*, IEEE Press, New York (1984).
5. Marco Listanti and Roberto Sabella, "Optical Networking Solutions for Next-Generation Internet Networks, *IEEE Communications Interactive*, September 2000; Daniel Blumenthal, "Routing Packets with Light," *Scientific American*, 96-99, January 2001.

# Quantum Network Considerations

Deborah Jackson  
David Gilliam  
Jonathan Dowling

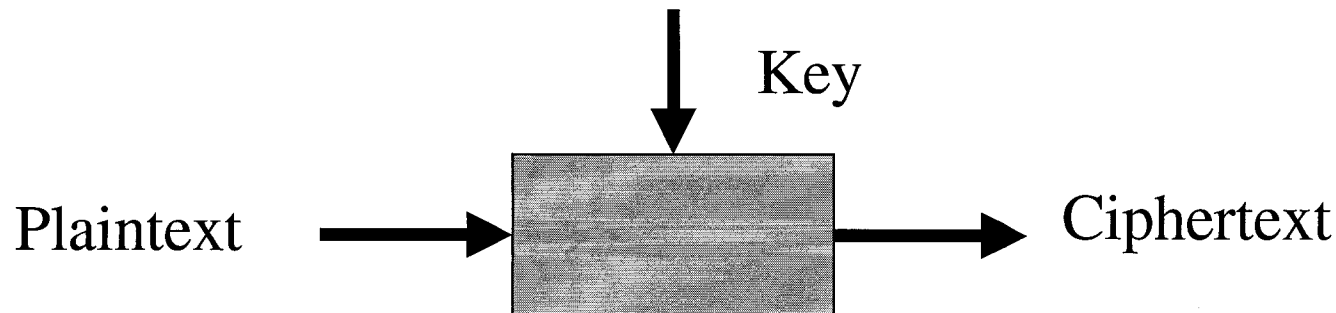
Jet Propulsion Laboratory  
California Institute of Technology  
Pasadena, CA

| Bit Value | Alice's<br>Polarizer<br>Settings   | Bob's<br>Polarizer<br>Setting  |
|-----------|--|--|
| 0         |   |   |
| 1         |  |  |

# Drivers for QKD Implementation **JPL**

---

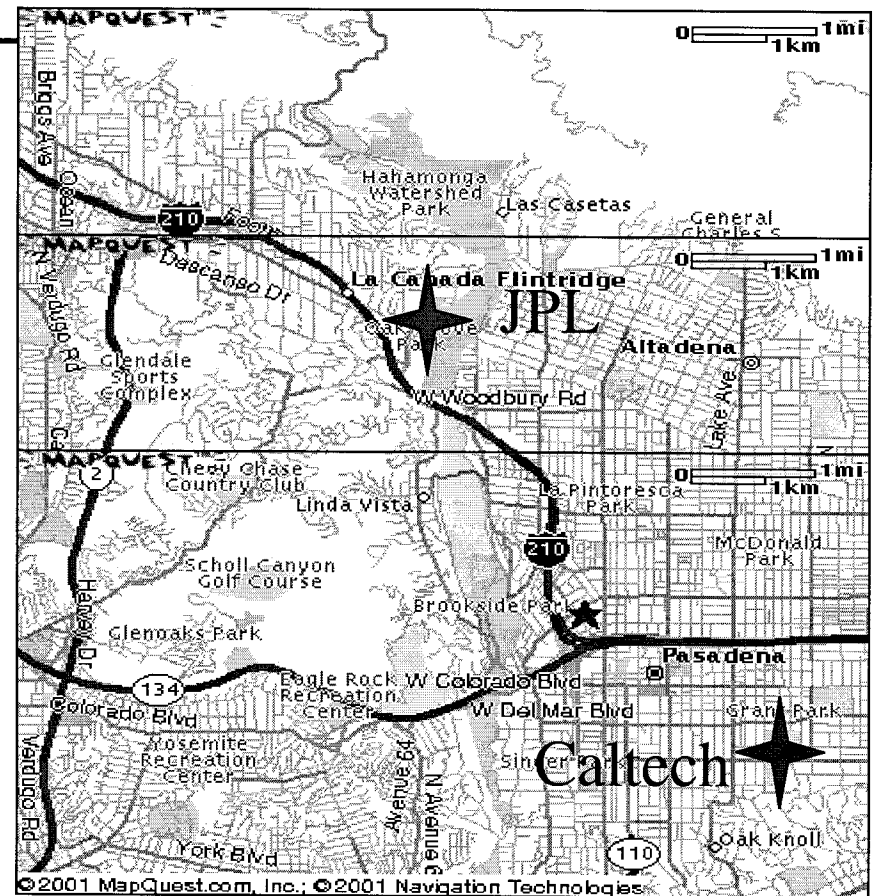
- Key exchange weakest part of crypto procedure
  - Symmetric => Asymmetric
- Impact of computational trends
  - Networking through the internet provides easy access to computational power for deciphering encryption algorithms.
  - Onset of quantum computers and other parallel processing methods attack confidence in most algorithmic encryption methods.
- Solution: QKD + Vernam Cipher = One Time Pad



# Buzz Words

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

**JPL**



LAN ~ University campus  
(approx. 1-5 km)

03/13/2001

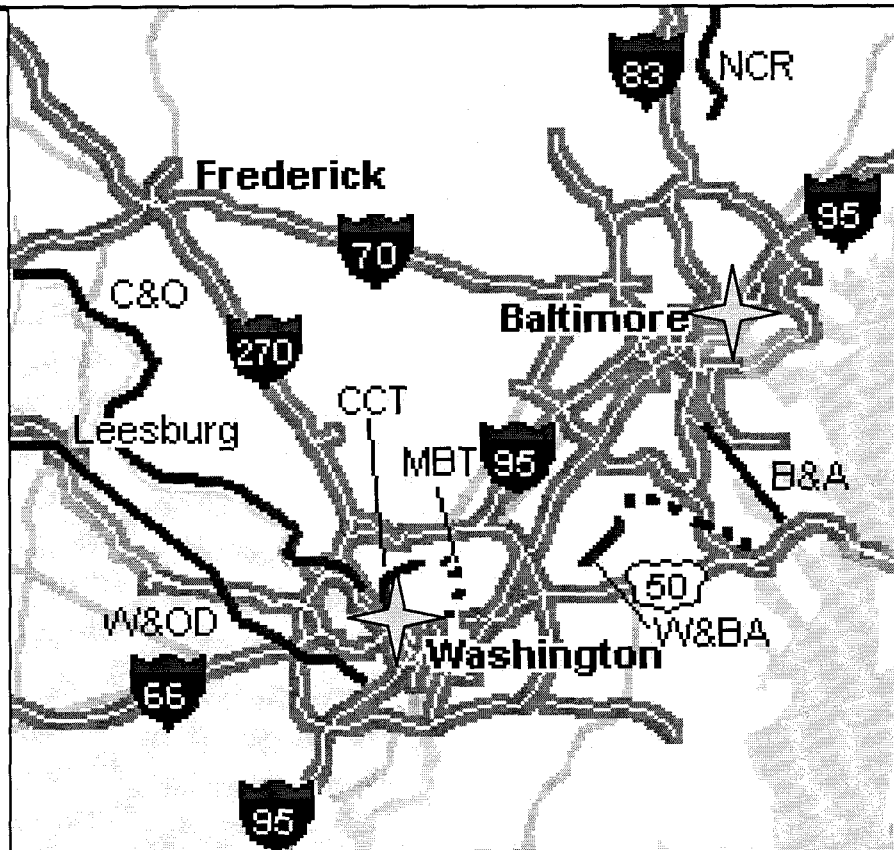
MAN ~ City size  
(approx 20-30 km)<sub>4</sub>



# WAN's

LANL Demonstrated point to point QKD over 49 km distance.

JPL



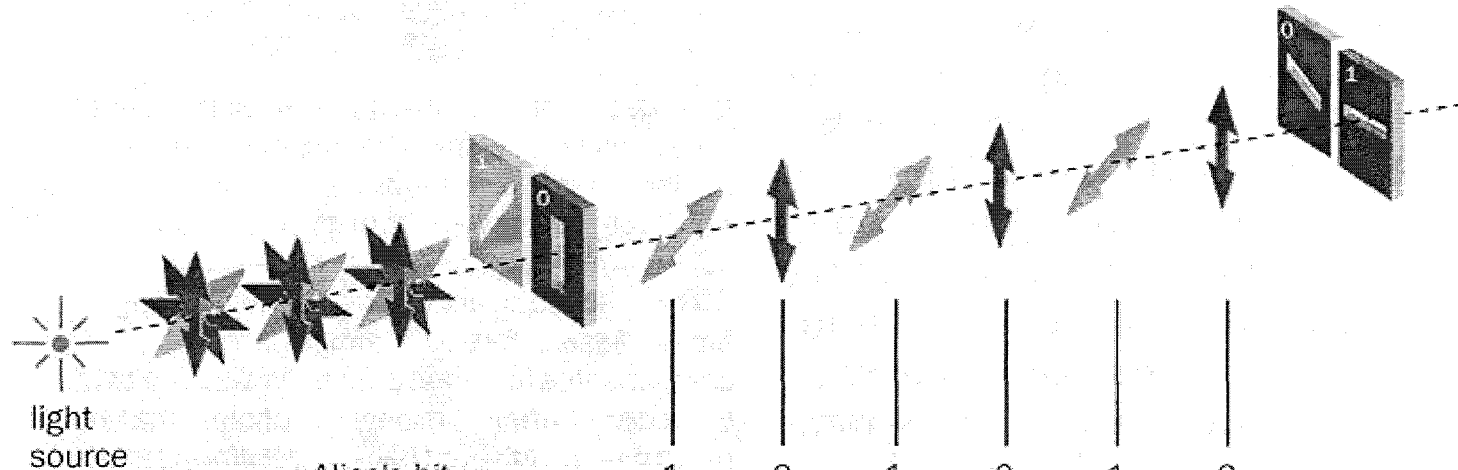
□ Baltimore to Washington => WAN scale distances.

□ Technology capability exists today to implement quantum LAN's and MAN's.

□ Challenge to use existing infrastructure.

Window of opportunity exists to define qubit requirements.

# 1 Cryptography with polarized light



IPL

|                      |      |      |      |   |      |      |
|----------------------|------|------|------|---|------|------|
| Alice's bit          | 1    | 0    | 1    | 0 | 1    | 0    |
| Alice's polarization | +45° | V    | +45° | V | +45° | V    |
| Bob's polarization   | -45° | -45° | H    | H | H    | -45° |
| Bob's bit value      | 0    | 0    | 1    | 1 | 1    | 0    |
| Bob's results        | N    | N    | Y    | N | N    | Y    |

Quantum cryptography is a way of generating a shared key to encrypt and decrypt a message with absolute secrecy from a sequence of bits (row 1). In the B92 protocol, Alice has two filters that can linearly polarize photons vertically (V) or at +45°. For each photon she sends through free space, she chooses one of these filters at random (row 2). Bob has analysers that can measure photons that are polarized in the horizontal (H) or -45°. Every time he expects a photon to arrive, he selects one of the polarizers at random (row 3) that correspond to bit values (row 4). He records whether or not he detects a signal and communicates this information to Alice over a public channel (row 5). Alice and Bob only retain the bits for which Bob detected a photon and they use these as a secret key. Bob will never detect the photon if he selects an analyser that is incompatible with Alice's polarizer (columns 1 and 4). In the case where he does chose a compatible analyser, he has a 50% chance of detecting the photon (columns 2, 3, 5 and 6).

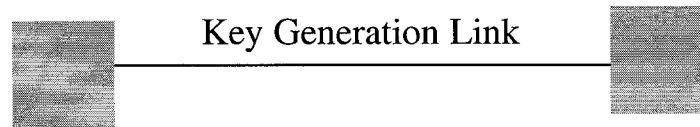
# 2-node QKD Key Generation Sequence

---

**JPL**

Alice

Bob

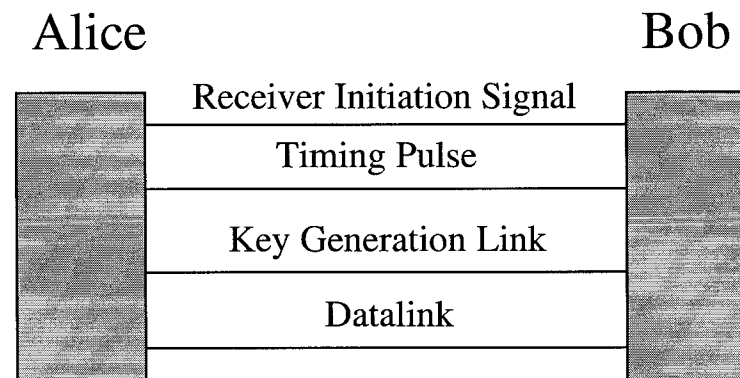


- QKD demonstrated over 49 km of dedicated experimental fiber by LANL.
- British Telecom demonstrated over 30 km of datalink; no degradation of QKD signal.

# 2-node QKD Key Generation Sequence

---

**JPL**

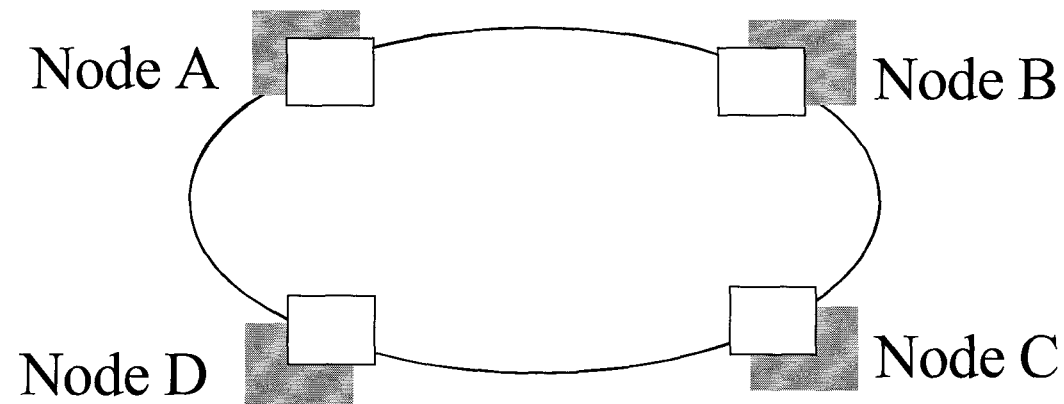


- Initiation broadcast from Bob indicates reception availability.
- Timing pulse from Alice provides reference for gated detection of photon.
- Alice generates photons through a random polarization; Bob detects photons with random polarization.
- Alice and Bob compare notes via communications on a data link to mutually establish random keys.



# Qubit distribution in multiple node LAN

**JPL**

Quantum Internet    Testbed    Network



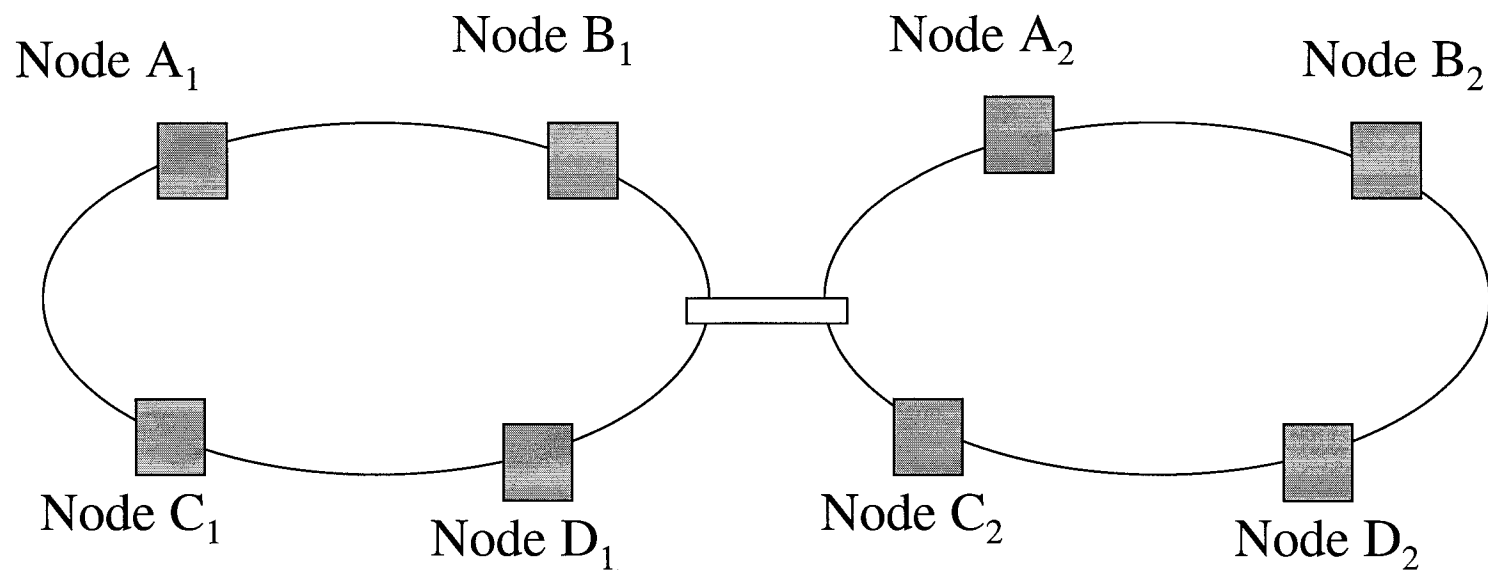
Legend:

-  Delay loop interface for timing control
-  Quantum computer or experiment at the node

Additional control functions needed:

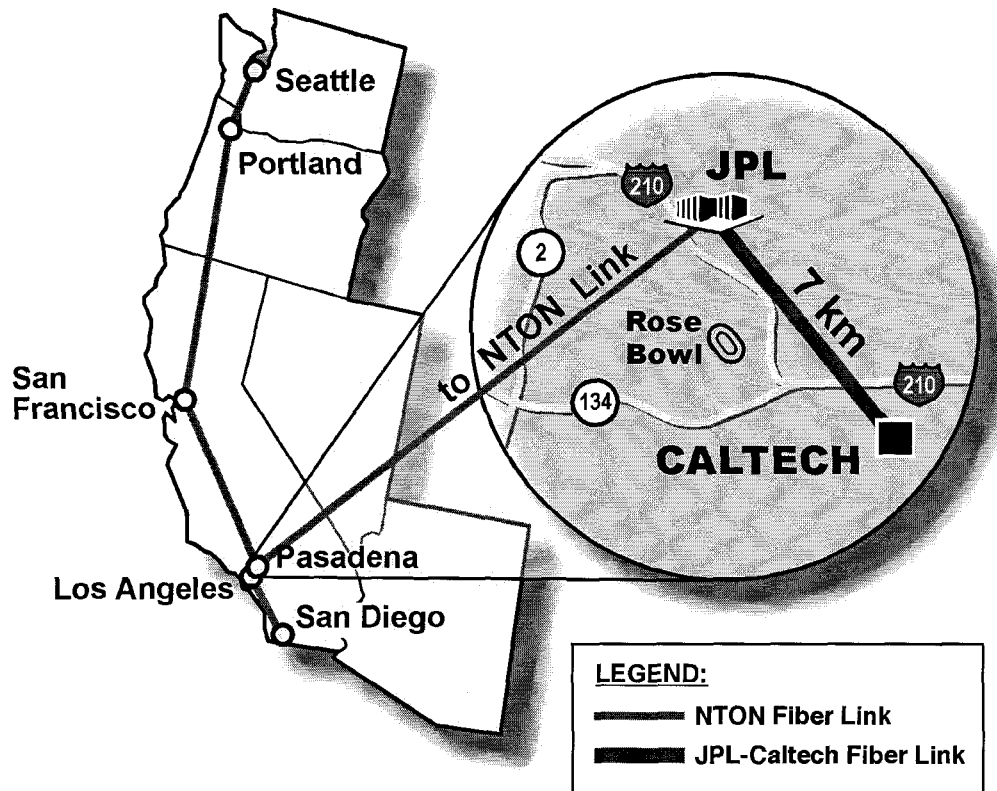
- Authentication protocol
- Dis-associated routing header

# Scaling up to Larger N



# Conclusions

**JPL**



- 12 strand single mode dark fiber between JPL and Caltech
- Testbed labs and offices are linked by single mode dark fiber
- JPL resides on one leg of the National Transparent Optical Network (quantum repeaters required)

## Example of (Quantum) Cryptography

- Alice and Bob generate shared key material (random numbers) using **single photon transmissions** of quantum cryptography over 14 km of optical fiber
- e.g. use of key for **"one-time pad"** encryption/decryption of short messages:

Sample of key material

|   |          |          |          |          |          |
|---|----------|----------|----------|----------|----------|
| B | 00001010 | 01111111 | 01010111 | 01011010 | 00010011 |
| A | 00001010 | 01111111 | 01010111 | 01011010 | 00010001 |
| B | 00000011 | 11100111 | 11011111 | 00000100 | 00001100 |
| A | 00000011 | 11100111 | 11011111 | 00000100 | 00001100 |
| B | 10110100 | 11101110 | 01110000 | 10100101 | 11111001 |
| A | 10110100 | 11101110 | 01110000 | 10100101 | 11111001 |
| B | 00110100 | 01001000 | 10000000 | 10111111 | 01010101 |
| A | 00110100 | 01001000 | 10000000 | 10111111 | 01010101 |
| B | 10111111 | 00000000 | 00100010 | 01011000 | 11011010 |
| A | 10111011 | 01000000 | 00100010 | 01011000 | 11011010 |

